

BEIS: Smart Data Research

Report: Liability

Lead author: Faith Reynolds

Co-authors: Sharon Cunliffe, Miles Cheetham, Gavin Starks

2020-03-31

REF: DGEN-SSD3-V2020-03-06



1





© Crown copyright 2020

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third-party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available from: www.gov.uk/bei

If you need a version of this document in a more accessible format, please email enquiries@beis.gov.uk. Please tell us what format you need. It will help us if you say what assistive technology you use. Any enquiries regarding this publication should be sent to us at: enquiries@beis.gov.uk

Commissioned by BEIS Produced by Dgen.net

Contents

Executive Summary	4
Where could common harms arise across Smart Data initiatives in	_
regulated sectors?	5
How should payment of any redress be apportioned between the data supplier and the third-party provider?	6
Summary of concepts	8
Overview	9
Common harms from data sharing and data sharing across sectors Liability and risk scenarios	10 12
Conclusions	15
Regulating Smart Data	16
Data initiatives in regulated markets	17
What are PSD2 and Open Banking?	20
PSD2	20
Open Banking	22
What is GDPR?	23
Mapping regulatory protections to risks	24
Conclusion	26
Redress	28
Current redress processes	28
Types of financial redress	29
Participants in the data chain Apportioning liability between Controllers	29 32
The data chain	36
Preconditions for redress	41
Conclusion	42
Biographies	44
Appendix:	46
GDPR principles, data rights and triggers	46
GDPR Principles	46
Data Rights under GDPR and their trigger points:	47
Glossary & terminology	51

Contents 3

Executive Summary

Our primary recommendation is to:

Give sector regulators concurrent powers for data protection and create a statutory Data Ombudsman for complex, cross-sector data sharing cases.

This will require a number of supporting actions and initiatives.

- 1. Develop additional consumer protections and enhanced rights for consumers through a Smart Data Right.
- 2. Put in place an appropriate trust framework to allow regulated actors to safely share data with other regulated parties.
- 3. Put in place a Smart Data Standard to allow consumers to share their data safely with Third Party Providers (TPPs).
- 4. Refine the proposed Smart Data Standards by
 - a. Requiring accreditation of providers to the same standard required for Account Information Service Providers (AISPs) under PSD2
 - b. Codifying the tenets of a 'Data Sharing Agreement' in the Standard, for instance, data minimisation, termination of data sharing
 - c. Setting out implementation requirements including Key Performance Indicators (KPIs)
 - d. Considering the powers required by regulators and delegates (e.g. Implementation Trustee) to require conformance to the Standard
 - e. Putting in place a regime of fines and sanctions for firms who consistently fail to meet the required standards
- 5. Consider creating a Smart Data Consumer Agreement to address other risks to consumers that have been identified. This could include:
 - a. The provision of consent management tools
 - b. A right to free, timely, accessible, individual redress
 - c. A responsibility for the ICO to undertake a consistent public information campaign about data rights, Smart Data and access to redress
 - d. TPP and 'Other Parties' right/responsibility to test their algorithms against a publicly held dataset
 - e. A duty on TPPs to put the consumer's interests before its companies to whom it onward shares data
- 6. Create a new architecture for Smart Data that learns from PSD2 but does not replicate it. This could bring Third Parties (Not Providing AIS) and Technical Service Providers (TSPs) into the regulatory perimeter. This will simplify the types of participants and make for a more manageable framework.
- 7. Explore the concept of loading liability for the onward share data chain onto TPPs so that they become responsible for managing traceability and the conduct of firms to whom data is onward shared. This could

- cause some natural reduction in the complexity of data chains and make apportioning redress easier. (However, this may impact innovation).
- 8. Provide for a single Dispute Management System to facilitate firm resolution of problems.
- Explore giving sector regulators concurrent powers for data protection so breaches of GDPR (including data breaches) can be addressed by sector ombudsmen.
- 10. Investigate the possibility of extending the regulatory perimeter to include sector data used by parties outside the regulatory perimeter.
- 11. Assess the merits of a single, statutory Data Ombudsman for complex, cross-sector data sharing cases.

This briefing provides a consideration of two questions posed by BEIS:

- 1. Where could common harms arise across Smart Data initiatives in regulated sectors?
- 2. How should payment of any redress be apportioned between the data supplier and the third-party provider?

These are complex issues and to address them we detail current thinking and provide pointers to areas for further consideration and research.

Where could common harms arise across Smart Data initiatives in regulated sectors?

There is a universe of risks which apply to Smart Data initiatives: new risks associated with opening up data; existing risks associated with using data; and risks which are exacerbated by the intelligence afforded by data.

Smart Data creates new operational and execution risks for firms as they seek to make data available, derive insights from it and automate new services. The over-emphasis in GDPR on Privacy Notices and disclosure to inform consumers is ineffective, creating the potential for consumer exploitation. Increasing reliance on data creates systemic risks and also challenges human rights to privacy and civil liberties. Data risks are often interlinked so that a mistake at a data provider creates risks downstream for other parties in the chain.

There are scenarios which may have a particular bearing on how liability and risk are spread across industry and consumer participants. These include, but are not limited to, where:

- There is no Smart Data Right
- There is no trust framework
- Participants play multiple roles in the data chain
- Data types blur definitions under GDPR
- There are no publicly available datasets against which to train algorithms
- There is a Smart Data Right in place but no easy access to redress
- There are complex data chains
- Data is shared outside the regulatory perimeter
- There is no access to a compensation scheme in the event a data provider or TPP goes bust

The Financial Conduct Authority, Ofgem and Ofcom's existing powers allow for a number of risks to be catered for through their focus on driving competition and protecting consumers. The Competition and Markets Authority and ICO are the cross-cutting regulators. All sectors have data-led initiatives underway. However, the most relevant are PSD2 and Open Banking. They provide a framework for the safe transfer of data which could provide learnings for Smart Data.

GDPR provides for consumer rights and protections when data is being shared. 'Explicit consent' for PSD2 and Open Banking only applies to the transfer of data¹. All data controllers in a data chain are also required to identify the legal basis for processing the data.

All three sector regulators provide for Alternative Dispute Resolution and access to redress. However, there is uncertainty about how redress would be provided for in the event of a data breach within or across a regulatory perimeter. In the event that the cases are passed to the ICO, a consumer's only access to redress would be through the courts which would be time-consuming and expensive. GDPR does not provide for free, accessible, timely, individual redress.

How should payment of any redress be apportioned between the data supplier and the third-party provider?

Before considering redress a liability framework is required. It is important to isolate who is liable in a data chain and what they are liable for. GDPR is the relevant regulatory framework for guidance. Data providers and TPPs are both data controllers and have similar responsibilities. However, there may still be risk as firms interpret the GDPR principles and their responsibilities differently. Firms could apportion risk through a 'data sharing agreement'. However, such a data sharing agreement would contravene PSD2 and potentially stymie competition as smaller firms try to negotiate arrangements with larger incumbents.

Improve traceability by shortening the data chain

A number of the elements of a data sharing agreement outlined by the ICO resonate strongly with the Open Banking Standard. This provides a foundation from which to build additional provisions into a Smart Data Standard which could codify such a data sharing agreement and remove the need for a contract. This could clarify what a data provider and TPP are responsible and therefore liable for.

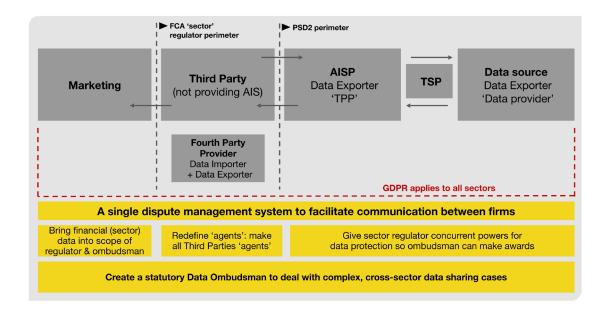
This would not solve fully for complex data chains where TPPs onward share data to Third Parties (Not Providing AIS). The longer the data chain becomes, the more difficult it is to identify where a data breach may have occurred because there is currently no mechanism for traceability. Where sector regulators are empowered to address data breaches and provide for redress, the practicalities of identifying the parties in the chain or requiring their co-operation when outside of the regulatory perimeter may make it impossible in practice.

¹ FCA Payment Services and Electronic Money, our Approach, June 2019 Para 8.54: "The interpretation of "consent" and "explicit consent" under data protection law should not be read across into the requirements under the PSRs 2017." https://www.fca.org.uk/publication/finalised-guidance/fca-approach-payment-services-electronic-money-2017. pdf

Preconditions for providing redress include how data itself is valued; how distress or reputational damage might be assessed; and the extent of the role data may have played in decision making by other providers. We recommend BEIS undertake research to explore these aspects further.

Create a statutory Data Ombudsman to deal with complex, cross-sector data sharing cases

Finally, the challenges may be best addressed by bold measures which consider giving sector regulators concurrent powers for data protection; creating a cross-sector Data Ombudsman for complex cases; bringing sector data into the purview of sector regulators (even where it is shared outside the regulatory perimeter); and re-defining data participant roles so the market is simpler and incentives are aligned to create better outcomes for firms and consumers. These potential measures would require further research with sector regulators and the ICO.



Summary of concepts

What is Smart Data?

In its Smart Data Review¹, BEIS explains that 'Smart Data' is an enhanced framework which extends the GPDR right to data portability to the real-time sharing of data via a set of standardised APIs. Data includes both product data (which includes new data sets such as performance data) and personal data.

What is a Smart Data Right?

The Smart Data Right would give consumers the right to port their data from regulated service providers in real-time to a Third Party Provider (TPP) in a safe and secure manner.

What is a Smart Data Consumer Agreement?

The Smart Data Consumer Agreement would confer new responsibilities on market participants and regulators to mitigate risks which occur in complex data chains. It extends and brings to life some of the key GDPR provisions.

What is a Smart Data Standard?

The Standard would be the suite of API standards, specifications and guidelines which underpin the technology across regulated sectors and ensure it is interoperable and consistent. It makes the transfer of data safe and facilitates consumers' control over their data.

What is a Smart Data Consent Standard?

The Consent Standard would codify the parameters of consent that the consumer has granted to the TPP in a consistent way across all sectors. The parameters would include those suggested in the ICO's 'data sharing agreement'.

These concepts require further research and definition.

¹ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808272/Smart-Data-Consultation.pdf

Overview

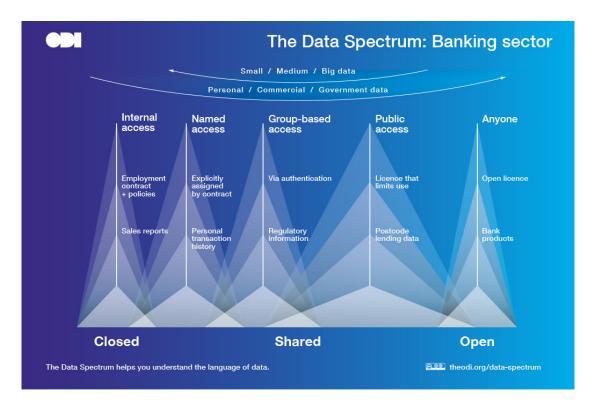
Where could common harms arise across Smart Data initiatives in regulated sectors? How should payment of any redress be apportioned between the data supplier and the third-party provider?

The Department for Business, Energy and Industrial Strategy (BEIS) is carrying out policy work looking at how best to enable and deliver Smart Data initiatives. These are sector specific initiatives aiming to facilitate the secure sharing of consumer data with third party providers, who use this data to offer innovative services for the consumer. This builds on proposals introduced in the Smart Data Review in June 2019.

The aim of this work is to inform the development of data portability initiatives in energy, telecoms and finance (with scope for applicability across further sectors). It considers how liability frameworks can be designed for individual or cross-sector initiatives in a way that encourages cross-sector interoperability so that consumers do not face different liability processes as they move between sectors and suppliers can rely on the same processes in different sectors. The key questions BEIS asked are:

- 1. Where could common harms arise across Smart Data initiatives in regulated sectors?
- 2. How should payment of any redress be apportioned between the data supplier and the third-party provider?

This brief assignment does not provide for an examination of liability in detail but highlights aspects for further consideration by BEIS.



Smart Data sits on the 'Shared' part of the Data Spectrum: it enables access to Shared Data² in a structured manner that enables many types of use and re-use.

Open Banking and Smart Data provide for greater personalisation, improved decision making and automation of services. The combination of shared data and technologies (e.g. algorithmic recommendation engines) can drive both efficiency and innovation. They support services which enhance life, simplify it and make it more convenient for many people across society.

Aggregated datasets can enable analysis that offers deep insights to individuals, communities, firms, regulators and government alike. Increased data-flows can facilitate the diversion of capital or government provision to where it is most needed; promise improved competition between companies; and allow the UK to compete more effectively with its international neighbours. It can enable new, relevant-time, granular analysis to reveal specific needs (e.g. sectoral market performance) and potentially unlock cross-sector analysis covering not only the regulated sectors specified for this work but also areas such as health & well being.

While the opening up of data creates opportunities, it also creates risks and the potential for harm.

Common harms from data sharing and data sharing across sectors

Data sharing already happens across sectors. The risk of harm occurs across the spectrum of activities from firms' own stewardship of data to its use by third parties and other parties in the data chain, including government.

Opening up access to shared data is not an end in itself. The overarching aim is for consumers to get value from their data by sharing it with TPPs. New risks occur when firms access data, store it and use it in the provision of services. Existing harms are simply likely to be exacerbated by the increased intelligence afforded by the data. However, old and new risks are not discrete but often interlinked, exacerbating risk and harm further.

The following graphic provides an example of some of the risks related to Smart Data. Further analysis can be found in the Appendix.

² The Data Spectrum: Defining Shared Data https://dgen.net/0/2019/05/06/the-data-spectrum-defining-shared-closed/

Examples of key risks not fully addressed by regulation

Access to shared data creates new operational & execution risks for firms	Use of data creates market and systemic risks	Wide sharing of data exacerbates consumer harm and risks to society
Access to data: is data easily accessible, accurate and up to date?	Nefarious actors: what are the incentives and routes in for illegitimate actors? How is fraud monitored and guarded against?	Value exchange: how should data affect the pricing of the product? Are there adequate price signals? Is the data
It systems: Do firms have the right systems in place to facilitate new tech? Are they resilient? Is investment proportionate?	What is the likelihood of cyber attack?	value exchange clear t Social scoring: do firms or government
Performance of technology: is the tech working, reliable and consistently available?	Product design features: are there tools to control data effectively? Can changes be enacted through the chain? Is there too little or too much friction?	create scores for people or businesses which reduce access, choice, social mobility, aspiration or democracy?
Capabilities afforded: is data minimisation possible?	Data driven automation: is it working as intended? Is it tipping the market?	Discrimination: is there negative discrimination which leads to bad outcomes for some groups of people?
secure in transit? Could data be intercepted in transit?	Misconduct and incompetence: do firms follow the rules and standards? Do they use the data for purposes other than the consumer agreed to?	Price optimisation: does personalisation lead to an increased loyalty penalty? Are consumer behaviours exploited?
Is data secure at all ends of the data chain?	Market discipline: what reporting and accountability requirements are there? Is there	Communications: are people and businesses aware of their rights and responsibilities?
Testing facilities: do firms have access to facilities for testing?	sufficient oversight, supervision and enforcement? Are there effective codes of conduct?	Incentivisation, distribution and point of sale: are consumers forced to share data? Are staff incentivised to make people share? Unfair teasers, commission bias, hollowing out?

The left hand side of the graphic focuses on risks associated with making data available as part of 'open access to shared data' or Smart data initiatives. From left to right, it highlights risks associated with firms' stewardship of data and the operational and execution risks; it considers the market or systemic risks that occur as data is used by third parties and data chains in the provision of services to consumers; it then exposes the harms that consumers may experience; and the risks that occur for society. In practice these risks interlink and overlap.

A particular challenge for consumers identified is the approach to disclosure through Privacy Notices. These form the main source of information for consumers about how their data will be used but the disclosure approach falls far short of what consumers need. There are no co-ordinated consumer communications to help consumers understand their rights, responsibilities and access to redress. And there is no requirement for data providers or TPPs to provide tools which may help people manage their consent or enact their data rights.

The focus of this work is on consumers in general but BEIS should consider the specific risks which occur for SMEs, to whom the principles and rights afforded by GDPR do not apply.

Key to understanding 'data issues' is to work out 'what can be done with it, by whom, and to what end'. In opening up data through Smart Data, BEIS must consider how it might address the downstream risks as well as the immediate operational concerns with making the transfer of data safe.

Liability and risk scenarios

By way of summary, the table below highlights some scenarios which could have a strong bearing on how liability and risk are spread across industry participants and consumers³:

Scenario	Potential considerations	
Where there is no Smart Data Consumer Right in place.	Firms could still seek to access the data via alternative methods such as screen-scraping. In such scenarios consumers could be forced to share credentials or divulge more data than they would like. With no easy access to consumer redress, consumers may carry more risk without recourse to protection in the event something goes wrong.	
	Without a Smart Data Consumer Right, data providers may block access to TPPs or only allow access to providers willing to enter a contract. This could discriminate against smaller players unwilling to bear the liability that may be pushed to them by larger providers. Alternatively they may sign unfair contracts, which in the event of loss they cannot fulfil.	

³ Examples included from FDATA, The Blueprint for Open Finance in the UK, 2018

Where there is no trust framework or 'single source of truth'	Without an adequate trust framework to identify regulated actors, a data provider may inadvertently share data with a nefarious actor. The consumer may lose out and the data provider may find itself liable in the event it should have done more thorough due diligence.
	The Open Banking directory provides a Directory which relies on the FCA's Register. For the Directory to operate effectively and avoid parties who have been struck off from continuing to access data, the sector regulator Register must also be updated regularly.
Where participants play multiple roles in the data chain	Data providers can also be TPPs. TPPs act as data providers when they onward share. TPPs may also act as TSPs for other providers. TSPs may provide services more akin to TPPs.
	Where participants play multiple roles in the data chain it may create conflicts of interest or confuse roles and responsibilities for apportioning liabilities.
Where data types blur definitions under GDPR	Open Banking allows for unredacted data to be passed on about silent parties. It also allows for "sensitive" (in GDPR terms) information to be inferred from transaction data.
	This could allow TPPs and others to use data in a way which exposes them to legal challenge if consumers or their associates suffer detriment.
Where there are no publicly available datasets against which to train algorithms	Where there are no publicly available datasets against which to train algorithms, TPPs may not be able to sufficiently test their products before they come to market or assess for inappropriate bias. The lack of such facilities creates downstream risks for consumers.
	The Global Open Finance Centre of Excellence aims to create such facilities in the UK.
Where there is a Smart Data Consumer Right in place but there is no easy access to redress, particularly in the event of a	Where there is a Smart Data Consumer Right in place (e.g. in the financial services market by way of Open Banking), consumers may still struggle to get redress particularly in the event of a data breach because sector regulators may not have powers to provide redress for breaches of GDPR. This may leave consumers carrying the can for firms' incompetence or misconduct.
data breach	Without clarity about how redress is calculated by a regulator and apportioned, firms may struggle to assess and access the correct liability insurance.

Where data chains are complex	Where there are several parties in a data chain the consumer may not be able to identify which party is at fault. On this basis, they may struggle to bring a complaint against any firm.
	If data providers and TPPs do not have in place sufficient audit processes, they may miss a data breach. In the event a consumer complains, a TPP's insurance provider may only pay out where liability can be established.
	Where an AISP uses a TSP to access data on its behalf, what happens if there is an interception as the data is in transit?
	Traceability is required to help clarify which participant holds the data for each customer at any given moment.
Where there is a Smart Data Consumer Right in place and there is right to redress, but the data is shared outside the regulatory perimeter.	Where there is a Smart Data Consumer Right in place and a right to redress, it is unclear how a consumer would access redress or how a regulator might apportion it where: • A TPP has accessed data from multiple regulated sectors • A TPP has onward shared the data with a fourth party outside the regulatory perimeter • A TPP has both accessed the data from multiple sectors and onward shared it to fourth parties outside the regulatory perimeter
Where there is no access to a compensation scheme in the event a data provider or TPP goes bust	Where there is no access to a compensation scheme, in the event a data provider or TPP goes bust as a result of a breach of GDPR the consumer may be left without recompense.

Conclusions

At a high level, opening up access to Smart Data creates a series of risks which could have the opposite impact to that intended by the policy. Simply mandating 'access to shared data' is unlikely to be sufficient in achieving the policy aims intended. A holistic, systemic approach must be taken to address the market: mitigations to the risks must be put in place by government, regulators and industry to guard civil liberties, avoid discrimination and exclusion and improve consumer engagement with their data and how it is used in the ecosystem. However, choosing not to regulate access to shared data also creates risks.

The economic analysis commissioned by [Ctrl Shift for Government] estimates that:

"the impact from personal data mobility enabled productivity and efficiency benefits of approximately £27.8bn increase in GDP. This is only one part of the value opportunity. The contribution to the economy that digital innovation driven by incumbents, new entrants, peer-to-peer markets and individuals themselves is likely to be significantly greater⁴".

Risks include reducing innovation and competition; increasing incumbency power (as they exploit their own datasets to the detriment of smaller or newer players); unregulated sharing of data by less secure or robust means (including screenscraping or reverse engineering); lack of regulatory powers to enforce good conduct; and inconsistent experiences for consumers across sectors and products, which frustrate their rights to data portability and leave them confused or more susceptible to nefarious actors.

Opening up and not opening up access to Smart Data both create risks and the potential for harm. We recommend that the best way to address these risks is to:

- Develop additional consumer protections and enhanced rights for consumers through a Smart Data Right so consumers can mobilise their data.
- Put in place an appropriate trust framework to allow regulated actors to safely share data with other regulated parties. This is likely to require research into emerging trust frameworks and approaches that could be deployed.

⁴ https://www.gov.uk/government/publications/research-on-data-portability

Regulating Smart Data

In its Smart Data Review (see also Consultation⁵), BEIS explains that 'Smart Data' is an enhanced framework which extends the GPDR right to data portability to the real-time sharing of data via a set of standardised APIs. Data includes both product data (which includes new data sets such as performance data) and personal data. We have focussed on personal data within the scope of this work.

BEIS Smart Data Review, 2019 says:

"Smart Data enables consumers, if they wish, to simply and securely share their data with third parties, to enable them to provide innovative services. The UK's data protection laws already give consumers the right to request that businesses provide their data to Third Party Providers (TPPs) in a commonly used format - this is known as the right to data portability. 'Smart Data' represents an extension of this right and provides an enhanced framework for sharing consumer data that allows for further innovation.

We consider key features of Smart Data initiatives to be:

- the immediate provision of data by the data holder to TPPs following a request from a consumer (rather than the one month permitted in the right to data portability)
- the use of Application Programming Interfaces (APIs) to share data securely, but only once the consumer has verified their identity and the TPP has received their express consent to do so
- where appropriate, an ongoing transfer of data between businesses and TPPs, rather than a one-off transfer
- adherence to common technical standards, data formats and definitions to ensure interoperability and to minimise barriers for TPPs
- provision of certain product and performance data, such as tariffs or geographical availability of services, in addition to consumer data, if necessary, to enable innovation

By combining consumer data with appropriate product and performance data, and by providing a seamless and interoperable framework for data sharing, innovators will be empowered to develop new ways for consumers to benefit from their own data."

In this Chapter we consider the regulatory regimes in place to deliver these aspirations, mitigate the risks previously explored and map the key gaps that remain.

⁵ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/808272/Smart-Data-Consultation.pdf

Data initiatives in regulated markets

Across the sectors of energy, telecoms and financial services, the regulatory framework focuses on driving competition to improve outcomes for citizens and protecting consumers. In both energy and financial services markets, regulators have a role to promote market integrity and sustainability, thus avoiding systemic risks. In energy and telecoms the regulators have a specific requirement to consider the needs of vulnerable people, while the FCA has published guidance on vulnerability for firms.

All three markets provide for Alternative Dispute Resolution (ADR) and regulators can require redress as part of their enforcement work. The Financial Ombudsman Service is a statutory ADR. Ofgem and Telecoms do not provide ADR directly but consumers can take their complaints to an independent ADR scheme (e.g. Energy Ombudsman and Communications Ombudsman).

Key cross-cutting regulators are the CMA and the ICO. The CMA ("Open Banking") Order created a regime for data sharing in retail banking. The CMA is active in considering competition in digital platforms⁶, digital markets⁷ and digital comparison tools. It is also seeking a change in powers to respond to increased digitisation and the need to protect consumers. The CMA is responsible for compliance with the Consumer Rights Act 2015 (CRA 2015) which provides for protection when goods or services go wrong. It has issued guidance on what good and 'unfair terms' look like.

The ICO is responsible for GDPR. Every company or sole trader that controls personal data must register with the ICO. There are 700,000 entities on the ICO register. In Appendix 2, we provide an overview of the principles of GDPR, data rights and when they are triggered. The ICO also provides guidance on data sharing through its Data Sharing Code of Practice. This has been consulted on recently and will soon be updated. It provides useful high level principles which we consider in the following chapter. It acknowledges that individual sectors may require more detailed codes⁸. As yet no sector codes have been developed for Open Banking. The Open Banking Implementation Entity is considering how nascent TPP Guidelines could be developed into an ICO accredited Code⁹. The ICO has Memoranda of Understanding in place with all three sector regulators to enable closer working relationships

The Centre for Data Ethics and Innovation (CDEI) is an independent advisory body set up and tasked by the UK Government to investigate and advise on how to develop a governance regime for data driven technologies to maximise their benefits¹⁰.

All regulators are actively involved in data-driven initiatives in both policy and practice.

⁶ https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study

⁷ https://www.gov.uk/government/news/cma-launches-digital-markets-strategy

⁸ https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

⁹ https://assets.publishing.service.gov.uk/media/5e398d5840f0b609278cd388/Trustee_Roadmap_Proposal_to_CMA_FINAL__-_200203.pdf

¹⁰ https://www.gov.uk/government/organisations/centre-for-data-ethics-and-innovation/about

Financial Services

The FCA is responsible for compliance with PSD2 and overseeing the UK's enabling legislation, the Payment Services Regulations 2017 (PSRs 2017) It works closely with the Open Banking Implementation Entity on the Open Banking standard which we explore below. It recently instigated a Call for Input into Open Finance and whether the concept of Open Banking should extend to other parts of the financial services industry. In their 20/21 business plan they committed to focusing on areas where they see potential for enduring harm.

Their aim is to ensure

"consumers are offered fair value products in a digital age, as use of consumer data and behaviour through digital channels increases, and with it the risk that consumers are not treated fairly in the pricing and other terms they receive" 11.

It has a year-long collaboration with the Alan Turing Institute on Al transparency. It has also extended its own data analytics capacity.

The Department for work and Pensions (DWP) and the Money and Pensions Service (MAPS) is working on the Pensions Dashboard. This will enable people to access their pensions information online, including their State Pension, and to see it in one 'dashboard'. A voluntary industry initiative is underway at The Investment and Savings Alliance (TISA) to develop APIs for Open Savings & Investments. The initiatives are both at an early stage but complement the FCA's work on Open Finance.

Energy

Ofgem has launched the MiData initiative which follows on from extensive change in the energy sector, providing consumers access to near real-time information about their energy usage. This is part of its wider work to promote more effective use of data. Ofgem has initiatives underway to facilitate industry coordination around data best practice to promote competition and transparency in the energy market, as well as lowering barriers to the innovation of new and better products and services. It is part of the Energy Data Taskforce which has made a series of recommendations including increased digitisation of the energy sector and maximising the value of data through improved infrastructure and standards¹².

Another relevant regulatory initiative is Ofgem's MiData for Energy and the Data Communications Code which underpins the Smart Metering initiative and gives rights to Third Parties (TPs) to access consumer energy data with their consent.

^{11 2020-21} Business Plan, FCA, 2020, https://www.fca.org.uk/publication/business-plans/business-plan-2020-21.pdf

¹² https://www.ofgem.gov.uk/about-us/ofgem-data-and-cyber-security

MiData in energy project1

Currently, there is no standardised way for energy consumption data to be shared with third parties. So when consumers want to get a new tariff quote or switch energy suppliers, they have to manually input their consumption data using information from a past bill or online account or to estimate it; which can mean consumers pay more for their energy than they should.

The MiData in energy project, led by Ofgem (with BEIS) is looking to replace the manual process with a standardised technology-based method for third parties (TPs) to access consumer data. This will include:

- a dictionary to define the language around data fields², integration mechanisms, security (including security tokens) and customer experience;
- an accreditation framework for TPs using midata (as TPs will operate outside of Ofgem's licensing framework);
- robust operational arrangements to monitor compliance and allow iterative evolution of midata; and
- a new Standard License Condition (SLC) to require all domestic gas and electricity energy suppliers to adhere to the MiData framework

As part of the consultation process, stakeholders have raised the need to clarify responsibility and liability where things go wrong when sharing energy data – for example between Ofgem and ICO³. Ofgem is currently considering delivery options for the MiData framework.

¹ https://www.ofgem.gov.uk/gas/retail-market/market-review-and-reform/midata-energy-project

² This may involve aligning data questions between MiData and the Smart Metering Data Privacy Framework

³ https://www.citizensadvice.org.uk/Global/CitizensAdvice/Energy/Energy%20Consultation%20responses/CitizensAdviceResponsetoMiDataEnergyConsultation.pdf

Telecommunications and Digital

Ofcom follows open data principles, making the data it collects and creates available to the public wherever possible¹³. Its open data covers media literacy, broadcast, ondemand, postal, telecoms, broadband and spectrum.

Ofcom has publicly discussed the challenges of regulating online in the past and has conducted research into this area¹⁴. In April 2019, the Government set out its thinking for a new regulatory framework to improve consumer safety online, including the creation of an independent Online Harms Regulator¹⁵. In February 2020, Ofcom responded positively to the Government's indication that it was minded to appoint Ofcom in this role¹⁶.

In a related initiative, the Report of the Digital Expert Panel on Unlocking Digital Competition recommended the creation of a Digital Markets Unit (DMU) - a new unit focused on businesses designated as having 'strategic market status', either as part of the CMA or Ofcom, or an independent body linking the two. In July 2019, the CMA published its Digital Markets Strategy document which took forward the establishment of the DMU and confirmed that its aims would include a code of conduct, and other possible remedies, not limited to data but including data interoperability, data mobility, and data openness¹⁷.

There are a range of relevant initiatives being undertaken by regulators. However, those dealing specifically with the current challenges associated with data sharing across the regulatory perimeter (e.g. the CMA's Digital Market Strategy) are still at an early stage of strategy formulation and have yet to formally publish operational proposals.

For the time being, the most obvious 'live' example to consider is PSD2 and Open Banking and their interaction with GDPR, which we describe below. We then provide a basic gap analysis highlighting areas for remediation.

What are PSD2 and Open Banking?

PSD2

PSD2 is the second European legislation which sets out to create a more integrated and efficient payments system in Europe; to protect consumers; and make payments safer and more secure through the introduction of Secure Customer Authentication (SCA). It also seeks to improve competition and innovation by levelling the playing field especially for new players. 'New' players include payment initiation service providers (PISPs) and account information service providers (AISPs) which are together termed 'Third Party Providers' (TPPs). PSD2 brings these TPPs into the regulatory perimeter and purview of the FCA.

¹³ https://www.ofcom.org.uk/research-and-data/data/opendata

¹⁴ See https://www.ofcom.org.uk/about-ofcom/latest/media/speeches/2018/tackling-online-harm and https://www.ofcom.org.uk/research-and-data/internet-and-on-demand-research/internet-use-and-attitudes/internet-users-experience-of-harm-online)

¹⁵ https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper-executive-summary--2

¹⁶ https://www.ofcom.org.uk/about-ofcom/latest/features-and-news/online-harms-regulator-response

¹⁷ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/814709/cma_ digital_strategy_2019.pdf

PISPs initiate payments from a consumer's account on their behalf with their 'consent'. In the event that something goes wrong with a payment (e.g. unauthorised fraud) the consumer can seek a refund directly from their bank, even if the fault is with the PISP.

AISPs facilitate the sharing and aggregation of 'account information' (i.e. the data you might see on your bank statement). AISPs are able to access the data from accounts from which payments can be made, which are also accessible online. AISPs can aggregate bank data from a range of different 'account servicing payment service providers' (ASPSPs, also known as banks and in our case 'data providers') into one place so that you can see a consolidated record of your transactions.

TPPs can onward share the data they collect from consumers with Agents that work on their behalf and with 'Other parties' (also known as Third Parties not providing AIS). These onward sharing relationships create complex data sharing chains which we explore more in the following Chapter. Suffice to say that once a consumer has shared their data with a TPP it could be passed to several providers, in the same way other data is.

Box 1

To become a TPP, firms must pass the FCA's licensing process. As part of this, AISPs need to prove that they:

- have robust systems and controls to keep data safe and secure
- use a specific 'trust framework' for identification towards the bank
- hold professional indemnity insurance
- have oversight and control over any technical service providers
- have processes to obtain explicit consent from the customer to access their transaction data
- are accountable to the customer if something goes wrong.
 In the UK that means having a complaints procedures in place, and that customers can escalate these complaints to the independent Financial Ombudsman¹.

A key safeguard in PSD2 is the requirement for the AISP [and PISP] to obtain explicit consent from the customer before accessing their account².

2 Jack Wilson, 2019, Ibid

¹ Customers and the Data Chain, Jack Wilson, 2019 https://blog.truelayer.com/customers-and-the-data-chain-aisps-and-tsps-e7343f93540

Regulatory technical standards for SCA under PSD2 set out how the secure communication between TPPs and ASPSPs should happen. It also makes provisions for how consumers should identify themselves to their ASPSP and 'authenticate' a data share. ASPSPs must provide a mechanism by which TPPs can access the data. Ideally they should do this through a 'dedicated interface' (usually APIs)¹⁸. If they meet the standards required by PSD2, they may be exempt from providing an additional 'contingency' or 'fallback' mechanism. The contingency or fallback is the 'modified consumer interface' (usually 'screen-scraping plus'). Firms may use their own proprietary APIs to provide a 'dedicated interface' or the Open Banking Standard.

Open Banking

Open Banking is a remedy for failings identified by the CMA in the personal and business current account market. It requires the UK's largest 9 banks to put in place API standards to enable consumers and SMEs to share their data securely with TPPs. It builds on PSD2 by requiring banks to facilitate data-sharing, where the consumer consents. Additionally, Open Banking provides a 'dedicated interface' and a single set of standards for all firms to follow. This creates consistency in the technology and allows TPPs to access consumers' accounts more easily.

The Open Banking Implementation Entity is responsible for delivering the Open Banking Standard. The Implementation Trustee oversees the banks' implementation. A key learning from Open Banking is that standards require consistent implementation and additional supervision is required for firms to ensure conformance to the standards. Non-conformance can create significant risks including security risks.

Unlike PSD2 which is relevant to all 'payments accounts accessible online', the CMA Order scope is directed to personal and business current accounts. However, the Open Banking standards have been designed to deliver against the requirements and scope of PSD2.

The design of the Open Banking standards means that a consumer does not need to share their personal security credentials with the TPP when they authenticate, unlike the 'fallback' or 'contingency' method which requires consumers to hand over their credentials to the TPP so that it can use them to access the consumer's account.

The banks' conformance to Open Banking standards, API availability, performance and reliability has caused considerable problems for TPPs. Exemption from providing a 'fallback' was supposed to act as a regulatory lever to get firms to conform to a dedicated interface. However, this has not been sufficiently effective. A better approach to driving the right outcome may be through fines and/or sanctions (for instance a firm whose APIs are not operating properly should not be able to access others' APIs to support provision of its own TPP service).

Open Banking also requires the largest banks to make available certain product, branch data and service quality data over the APIs. This allows TPPs to offer personalised services based on the consumer's own shared data and this new 'open' data retrieved from banks. (TPPs do not need to seek 'consent' to access open data).

18 https://www.fca.org.uk/firms/exemption-psd2-contingency-mechanism

Both PSD2 and Open Banking require 'explicit consent' for the secure transfer of data from the 'ASPSP' (bank) to the Third Party. 'Explicit Consent' for PSD2 should not be confused with 'consent' under GDPR. 'Explicit consent' under PSD2 relates only to the transfer of data to the TPP. Before accessing the consumer's data a TPP must have identified their legal basis for processing the consumer's data under GDPR.

The CMA required that customer redress mechanisms for the Open Banking Standard also be put in place. The Open Banking Implementation Entity has provided for a Dispute Management Service which allows firms to work out liability in the event of a consumer claim. However, it has not provided for a specific redress mechanism for breaches of GDPR.

What is GDPR?

GDPR provides for the relevant regulation in EU law on data protection and privacy. In the UK, the GDPR has been enhanced by the updated Data Protection Act (2018) (DPA 2018). "The GDPR aims primarily to give control to individuals over their personal data and [...] contains provisions and requirements related to the processing of personal data of individuals (formally called data subjects in the GDPR)"¹⁹.

The scope of GDPR protection does not extend to SMEs or corporates.

GDPR gives rights to the ICO to levy heavy fines on firms who fall foul of its rules. However, it does not provide individuals with easy, free or timely access to individual redress. Consumers may complain to the ICO which can require firms to put things right. However, should an individual wish to pursue individual financial redress, under current law, this would only be possible through the courts. This is in direct contrast to other regulated sectors where both ADR and access to redress without recourse to the courts is possible.

The ICO sets out a series of data protection principles which all Controllers must comply with for GDPR. GDPR is a principles based regulation which confers important rights for consumers:

- 1. The right to be informed (Privacy Notice)
- 2. The right to object
- 3. The right to deletion/ erasure (also known as the right to be forgotten)
- 4. The right to rectification
- 5. The right to data portability
- 6. The right to restriction
- 7. The right of access (i.e. a subject access request, or SAR)
- 8. Rights in relation to automated decision making and profiling

Appendix 2 outlines the GDPR principles, rights and how they are triggered. Some of these rights are qualified whilst others are absolute and therefore it is imperative that consumers understand what rights can be exercised and when. This information is usually provided through the Privacy Notice.

19 https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

The huge number of firms subject to GDPR makes it very difficult for the ICO to authorise or supervise this number of firms easily. The effectiveness of its regulation relies on strong enforcement against a smaller number of key firms to communicate a sufficient deterrent to others. This allows room for general low level misconduct. For instance, despite clear guidance on how firms should communicate with consumers, the reality suggests that firms do not apply this in practice. It may be helpful to consider how sector regulators can provide more supervisory support for data protection as part of their role in Smart Data.

Giving sector regulators concurrent powers for data protection may be more effective than MOUs.

Mapping regulatory protections to risks

The existing regulatory focus on driving competition and good outcomes for consumers means that subject to agreement from regulators:

- A number of risks are well-understood and catered for (e.g. distribution risks); or
- Existing powers could be applied to new problems relating to the use of data (e.g. aspects of the data value exchange).

As DCMS notes:

"GDPR only creates a right to data portability, it does not enable it or create the structures to support value generation from personal data portability. Furthermore, there are new risks. In the absence of a safe and secure environment for the sharing of personal data, the new rights that individuals have over their data introduce new potential hazards for both them and the organisations with which they interact"²⁰

Our analysis shows that current regulations do not adequately address operational, execution, market, consumer or society risks:

- There are no suitable regulatory provisions for the safe transfer of data (as noted by the Smart Data consultation)
- Where there are provisions (e.g. PSD2 and Open Banking), these are complex and limited in scope. We explore data chains further in the following Chapter.
- The provisions of GDPR are strong but supervision is a challenge. The practical risk based application by firms of GDPR provisions falls far short of what consumers need and can reasonably engage with.
- There are no requirements for consent management tools to provide transparency about how consumer data is used or to enable consumers to enforce their data rights in a standardised way in realtime.
- There is no general education programme for consumers to help them understand their rights or how they can safely share their data through initiatives like Open Banking, nor a requirement on any regulators to provide one.
- ADR schemes exist for regulated sectors. There are gueries about

20 https://www.gov.uk/government/publications/research-on-data-portability

the extent to which consumers could pursue redress for data breaches through their sector regulator and ombudsman. There is also a query about how a sector regulator may take enforcement action against a firm in the event of a data breach for instance. Would the FCA remove a license for an AISP if they can be shown to have been part of a data breach identified by the ICO? There is also a lack of regulatory certainty in terms of how to deal with redress in the case of data breaches in particular²¹.

 The increase in high quality datasets such as those provided by Smart Data, create increased opportunity for surveillance which could have a detrimental impact on privacy and civil liberties.

If these issues are not addressed, Smart Data may have the opposite effect of what was intended.

Applicable regulatory and policy provisions

operational & execution r	risks for firms mark	ket and systemic risks	_	of data exacerbates n and risks to society
Operational risks	Execution risks	Market / systemic risks	Consumer harm	Societal risk
Provisions in PSD2 and the CMA Order for retail banking Data Communications Code and SEC for Smart Energy Ofcom Digital Markets Review and Online Harms ICO Data Sharing Code of Practice (to be updated)	Policy work underway but no specific rules GDPR principles apply but require interpretation	GDPR principles apply but low barriers to entry and limited supervision ICO has strong enforcement powers ICO Data Sharing Code	Consumer Rights Act requires services to be 'fit for purpose' 'Informed consent' and disclosure requirements do not have the desired impact No requirement to provide consent management tools GDPR does not state specifics of how firms should make rights achievable by consumers in real-time	There is no cross-cutting responsibility for communicating consumerights and responsibilities Complaints are difficult to pursue and there is no right to redress Centre for Data Ethics advisory only

²¹ https://www.ftadviser.com/regulation/2018/02/08/fca-in-talks-to-iron-out-data-protection-rules/

Conclusion

"If universal data mobility is to happen, it will have profound implications everywhere. Basic, simple rights for the individual will be needed and the legislative and legal structures to protect them"²²

There are a range of risks for Smart Data across the value chain which current regulatory protections do not cater for. PSD2 and Open Banking provide an example of how some operational risks can be addressed. However, Open Banking on its own is not sufficient to cater for other execution, market, consumer or society risks that opening up data creates.

We recommend that BEIS:

- Explore giving sector regulators concurrent powers for data protection so breaches of GDPR (including data breaches) can be addressed by sector ombudsmen through existing ADR schemes
 - This would require a thorough review of existing sector regulator data powers and working approaches to assess what risks they can protect for within their current regimes; consider what changes they may need to make to working practices (including joined up working with the ICO); and provide BEIS with a gap analysis. This could build on existing MOUs between regulators²³.
 - This should also include a review and consideration of an amendment to of the CRA 2015, which could provide for consumer redress in the event of data breaches
- Assess the merits of a statutory Data Ombudsman Service for complex, cross-sector data sharing cases. This could be part of the ICO or potentially any new Digital Markets Unit.
- Provide for a Smart Data Right so consumers can mobilise their data in real-time through the Smart Data API Standards, as suggested in the Smart Data Review.

²² Jeremy Wilson, Vice Chairman, Barclays Corporate Bank, quoted in Data Mobility Report, 2018

²³ https://www.ftadviser.com/regulation/2018/02/08/fca-in-talks-to-iron-out-data-protection-rules/

- Refine the Smart Data Standards:
 - Require accreditation of providers with their initial sector regulator to the same standard required for Account Information Service Providers (AISPs) under PSD2, as noted in Box 1. Once accredited, firms would simply need to register with additional sector regulators to access other datasets. Some further checks may be necessary where they access significantly more data or where it has been several years since their last authorisation.
 - Set out the key requirements for the APIs, providing for interoperability between sectors
 - Facilitate data minimisation in the design of the APIs and require the availability of accurate, comprehensive and real-time data
 - Set out the key requirements for their implementation including KPIs for their availability, performance and reliability, including reference to Customer Experience Guidelines (see our Consent paper)
 - Consider the powers required by regulators and their delegates (e.g. Implementation Trustees) to require industry conformance to the standards. This should include what is required of TPPs as well as data providers.
 - Put in place a regime of fines/sanctions for firms who consistently fail to meet the required standards (both data providers and TPPs)
- Consider creating a Smart Data Consumer Agreement to address other risks to consumers and society that have been identified (please also see our paper on Consent). Such an agreement might include:
 - A duty on TPPs to put the consumers' interests before its companies to whom it onward shares data and create a 'data facilitator' or 'data custodian' role for TPPs
 - A responsibility for the ICO to undertake a consistent public information campaign about data rights, Smart Data and access to redress
 - TPPs right/responsibility to test their algorithms against a publicly held dataset to achieve a minimum standard (for instance, see the Global Open Finance Centre of Excellence initiative)
 - The provision of consent management tools by TPPs which allow for consumers to enforce their GDPR rights in real-time across the data chain in simple and intuitive ways
 - A right to individual, timely, free and accessible redress in the event of a problem or breach of GDPR (provided for through sector regulators and/ or dedicated Data Ombudsman)

Redress

In a cross-sector data sharing ecosystem how should redress be apportioned?

In the first part of this work we have considered where common harms could arise across Smart Data initiatives in regulated sectors and how BEIS might consider addressing them. In this half we consider how payment of any redress might be apportioned between the data supplier and the third-party provider.

Before a redress process can be put in place, a liability framework is required. It is necessary to isolate who is liable in a data chain and what they are liable for. This brief assignment does not provide for an examination of liability in detail but highlights aspects for further consideration by BEIS.

By way of background, we explain the current redress processes and types of redress. We then turn to the roles of participants in the Open Banking and PSD2 data chain. We consider how responsibilities might be shared between these parties. We look at three different data sharing journeys and the nature and characteristics of data. We finish with some considerations for managing liability and redress in a cross-sector data sharing ecosystem.

Current redress processes

For the purposes of this work, 'redress' refers to the consumer dispute resolution (CDR) processes for resolving consumer-to-business (C2B) disputes.

"Effectively, CDR now provides a parallel system of justice for C2B disputes, with courts relegated to a peripheral role in many areas."²⁴

As noted by Gil et al²⁵, the use of CDR over court mechanisms for C2B disputes makes sense given the low value of most claims and the power asymmetry between consumers and large businesses. The Consumer Manifesto for Open Banking Consumer notes "people should have simple, free, quick access to help and redress" ²⁶.

In terms of redress, for breaches of GDPR, we have already noted that consumers would only be able to get redress through the courts²⁷. As noted by BEIS in its Consumer Green Paper, "consumers should be able to get redress when things go wrong and consumer rights are effectively enforced". Accessing redress through the courts is both complex, time-consuming and costly. This means very few consumers would be able to access redress.

One area we have not considered is how consumers can complain. This is an area for further research and consideration, especially in light of the complexity of data chains.

²⁴ C Hodges, I Benohr and N Creutzfeldt Consumer ADR in Europe: Civil Justice Systems (Oxford: Hart Publishing, 2012

²⁵ Chris Gill, Jane Williams, Carol Brennan and Carolyn Hirst, Legal Studies, Vol. 36 No. 3, 2016, pp. 438-463.

²⁶ https://www.openbanking.org.uk/about-us/latest-news/consumer-groups-create-manifesto-open-banking/

²⁷ https://www.which.co.uk/consumer-rights/regulation/gdpr-data-protection-act#multiple-routes-to-claim-compensation

Types of financial redress

Redress usually aims to put the consumer back into the position they were before the company made a mistake. Ombudsmen may require firms to take practical action to put something right that was wrong; make an apology; or offer a financial reward. In some cases a regulator may require comprehensive consumer redress as part of an enforcement action (e.g. PPI mis-selling).

Our focus is on providing for financial reward for an individual whose complaint has been successful.

Financial rewards may take a variety of permutations. The Financial Ombudsman Service (FOS) considers:

- Money awards where a consumers has lost out financially
- Awards for trouble, upset, distress or inconvenience. This may include pain and suffering or damage to reputation
- Interest awards which provide for interest that was paid that should not have been (e.g. in case of overcharging on a mortgage); interest on the money the consumer would have had access to if they had not been 'deprived'; and interest which accrues if there is unreasonable delay to settling the complaint
- · Other costs that the consumer reasonably incurred

In a cross-sector data sharing ecosystem, consideration would need to be given to ensure that rewards were calculated in a consistent way. The parameters and payments for redress would ideally be set at the same level or above the level of the most generous ombudsman.

This would ensure that, no matter which ombudsman provides redress, consumers get a consistent outcome.

Likewise, it should not require any regulator to diminish its existing redress process for data complaints. It may, however, raise standards for some ombudsmen.

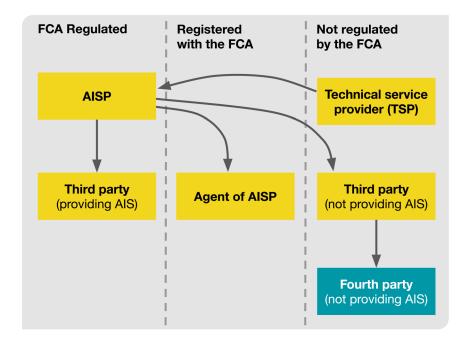
Further work is required to assess existing approaches to redress and how these could be harmonised for breaches of GDPR.

Participants in the data chain

PSD2 has created a complex network of providers in a data chain which could make apportioning redress complex. For redress to be apportioned an ombudsman must be able to identify the participant in the data chain.

Here we use the example of PSD2 to consider different potential market participants and their key responsibilities under PSD2. The graphic below (based on FCA December 2019²⁸) offers more guidance to firms.

28 https://www.fca.org.uk/firms/agency-models-under-psd2



The roles of the different parties are complex as illustrated below:

Participant type	Description and explanatory note		
	Regulated		
Data Source or ASPSP	The company or organisation that holds the consumer data to which the consumer consents the AISP (TPP) access.		
(Account Servicing Payment Services Provider. e.g. bank)	The bank must provide to the AISP the data it requests (in line with the law) without requiring additional consent from the consumer.		
	A bank cannot require a contract with a TPP to allow the TPP to access the consumer's data.		
TPP/AISP	Retrieves the consumer data from the data source.		
(Third Party Provider or Account Information Service	Provides consolidated account information to the consumer. They are responsible for compliance with the PSD2/PSRs 2017.		
Provider)	The AISP must display back to the consumer the data retrieved. They must do this in all journeys apart from where an Agent works on their behalf.		
TPP (providing AIS)	If a regulated AISP provides data to other firms that want to provide AIS, the other firm needs to be regulated for AIS as well. The information provided to a third party must also be provided to the consumer.		
	In the case where an AISP provides a service to another AISP both providers must display the data retrieved back to the consumer.		
	In this scenario, the first AISP is operating in a similar way to a TSP.		

Participant type	Description and explanatory note	
	Registered (with the FCA)	
Agent of AISP	Regulated AISPs (Principals) can have agents. An agent provides services on behalf of the principal. It cannot provide AIS on its own behalf. The principal must register the agent with the regulator (FCA).	
	In this case the Agent displays the data retrieved back to the consumer on behalf of the AISP.	
	The AISP is responsible for the Agent. Liability for a data breach is likely to rest with the Agent. However, it is possible the AISP may recover damages from the Agent.	
	Accesses consumers' accounts on behalf of the AISP. They obtain and process account information in support of an AISP but do not provide the information to the user.	
	If a firm does not display the information it retrieves back to the consumer, it is a TSP. TSPs do not fall within the regulatory perimeter. They are not able to access consumer's data without using the credentials of a regulated AISP.	
	Not regulated by the FCA	
Technical Service Provider	Accesses consumers' accounts on behalf of the AISP. They obtain and process account information in support of an AISP but do not provide the information to the user.	
	If a firm does not display the information it retrieves back to the consumer, it is a TSP. TSPs do not fall within the regulatory perimeter. They are not able to access consumer's data without using the credentials of a regulated AISP.	
Third Party (not providing AIS)	Where an AISP retrieved data from the consumer in compliance with applicable laws and regulations, it can pass account data to an 'Other Party' or Third Party Not Providing AIS (and not regulated for AIS).	
	The AISP must display back to the consumer the information it has provided to the Third Party Not Providing AIS.	
	Some examples where this may happen are credit scoring, mortgage applications or loan applications.	
Fourth Party (not providing AIS)	In the case where the Third Party (Not Providing AIS) onward shares the data to a fourth party, it is termed Fourth Party (Not Providing AIS). This would not be considered a transfer of data under the PSRs 2017 but would, instead be solely covered by GDPR.	
	An example of this is where a credit scoring company passes data to a loan company.	

Apportioning liability between Controllers

In the case of financial awards, BEIS questions how redress should be apportioned between the data supplier and third party.

When data is shared between parties (within or across sectors) the chain can be summarised as starting with the first Data Controller and moving through a series of Third and Fourth Parties also defined as Data Controllers. In the descriptions above, only the TSP would be considered a Data Processor unless they were to undertake activities appropriate to a Controller (e.g. categorisation of the data).

Under Article 82 of GDPR, consumers who have suffered damage as a result of a breach of GDPR bring a claim for compensation against a Controller or Processor. While the primary obligation is on the Controller, the Processor can also be held liable if it has not complied with its specific GDPR obligations²⁹.

In notes on the right to data portability, the ICO states that a data provider is not responsible for the processing of the data by the TPP. However the data provider is responsible for ensuring data is safely transmitted and to the right TPP³⁰.

All Data Controllers have the same responsibilities to comply with GDPR.

For instance, a bank (data provider) should ensure that it's data is accurate and up to date. If it were to share this with a TPP, the TPP (as a data controller) would also be responsible for ensuring the same data was accurate and up to date. However, the ICO states that,

"whilst there is no specific obligation under the right to data portability to check and verify the quality of the data you [the data provider] transmit, you should already have taken reasonable steps to ensure the accuracy of this data in order to comply with the requirements of the accuracy principle of the GDPR."³¹

²⁹ https://blogs.dlapiper.com/privacymatters/uk-liability-limits-for-gdpr-in-commercial-contracts-the-law-and-recent-trends

^{30 &#}x27;Do we have responsibility for personal data we transmit to others?' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

³¹ See' Do we have responsibility for the personal data we transmit to others?' Ibid

How can a TPP then rely on the data provided by the data provider, especially in cases where inaccurate information may have a significant impact? The ICO recommends 'data sharing agreements' to help controllers understand their respective obligations:

"Where you are acting with another controller as joint controllers of personal data within the meaning of Article 26 of the GDPR, you are required to set out your responsibilities in an "arrangement". This may be done by means of a data sharing agreement. Under the transparency requirements of the GDPR you must make the essence of the agreement available to individual data subjects. We recommend you do this in the privacy information you give to them."³²

Within Regulations 69 and 70 of the PSRs 2017, it states that no contract can exist between the ASPSP ('data provider') and TPP for AIS or PIS services. Were a bank to require a contract this would contravene the Directive. This is a desirable arrangement for Smart Data, as well as PSD2, because it facilitates a level playing field between participants and therefore innovation and competition. To require smaller firms to negotiate data sharing agreements with larger firms may put them at an immediate disadvantage. Therefore in terms of thinking about how liability is apportioned it may be helpful to consider how such data sharing arrangements can be codified by the Smart Data Standard.

The ICO makes a series of recommendations about what should be included within a data sharing agreement. These include:

- The purpose of data sharing
- Other organisations involved in the data sharing
- What data items will be shared
- The lawful basis for sharing (for GDPR)
- Inclusion of special category or sensitive data
- Access and individual rights of the data subject (consumer)
- Information governance arrangements (such as accuracy of data, the deletion of data, termination of data sharing and complaints management)
- Review periods for the agreement

The list of requirements resonates strongly with the Open Banking Standard and provides a foundation from which to build additional aspects into a Smart Data Standard.

³² https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

A summary analysis of some elements mentioned by the ICO are covered here:

ICO Recommendation	Does the OBS provide for this?	Summary analysis
Purpose	Yes but it could be improved	Purposes could be further codified to bring familiarity to firms and consumers; metadata could also be attached to the purpose as the data is passed through the chain (see our Consent paper)
Other organisations involved in data sharing	Only agents	There is currently a debate about whether it is anti-competitive for 'banks' to know the other Third Parties Not Providing AIS to whom TPPs onward share data.
		For instance, if a consumer chose to share data to access a mortgage, this could allow the data provider (e.g. bank) to use this information to target the consumer with mortgage offers.
		Further work could be done to consider how best to address issues like these in a regulatory data sharing context where data controllers may be in competition.
Data items shared	Yes	The Open Banking Standard allows for data minimisation through the clustering of data types.
Lawful basis for sharing	No	This is currently confused by the PSD2 requirement for explicit consent as the basis for transferring the data. TPPs therefore provide Privacy Notices separately.
		Again further work is required to consider how this might best be conveyed between the parties and whether it is still best to provide this in the Privacy Notice to the consumer.
Inclusion of special category or sensitive data	No	Further work may be required by BEIS to consider what types of special or sensitive category data could be passed to TPPs in different scenarios.
		PSD2 for instance forbids the passing on of credentials such as PIN to the TPP.

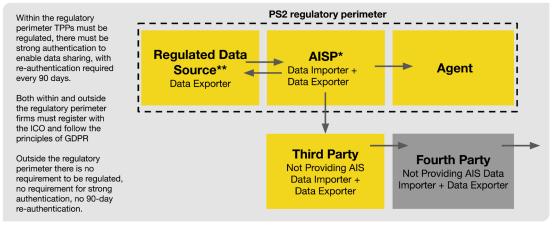
Access and individual rights of the data subject	No	Both data controllers would be able to action individual rights and thus it is unclear if this would be needed in the context of a Smart Data Standard. However, consumers need clarity about who they should complain to in complex data chains.
Information governance arrangements	Partly	The Open Banking Standard caters for a range of aspects here such as termination of the data sharing arrangement, dispute management etc. However, it could go further and set out how TPPs might rely on the accuracy of TPP data for example.
Review periods for the agreement	Yes	The Open Banking Standard is regularly reviewed. It would therefore be possible to review a Smart Data Standard regularly to check whether it is fit for purpose.
		However, it is worth noting that significant changes require implementation and build costs. As such in setting out a Smart Data Standard consideration should be given to what must be achieved through the technology itself and what can be achieved through alternatives such as Guidelines.

We would recommend that as part of its further consideration of Smart Data BEIS consider how it can use the Smart Data Standard as a vehicle for codifying aspects of a Data Sharing Agreement as set out by GDPR.

The data chain

As we have shown above the data chain is often longer than a data supplier and third party. Many third parties onward share data to fourth parties. The UK interpretation of PSD2 has focused on the importance of the role of the TPP as a consumer-facing entity. This aims to provide clarity to the consumer about which provider has accessed their data for what service. In practice, the brand the consumer is likely to be most familiar with is the one providing the ultimate product or service the consumer is buying.

One learning from Open Banking is that AISPs are increasingly acting as 'data facilitators' between consumers and their agents, or between consumers and Third Parties Not Providing AIS. This has implications for the regulatory role of AISPs in PSD2 and how they might better provide a clear consumer-facing offering which adds value.



- * AISP may use a TSP (which does not have to be regulated) in order to access the consumer's account at the data source.
- ** A regulated Data Source like a bank may also be authorized to act as an AISP. Banks can therefore also be TPPs.

Third Parties and Fourth Parties Not Providing AIS outside the regulatory perimeter are not required to:

- prove themselves fit and proper to regulators before accessing a consumer's data
- undertake Secure Customer Authentication before receiving the data
- undertake re-authentication to check for security purposes or check the consumer's continuing interest in the service (which guards against disengaged consumers unwittingly sharing data).

They are required to register with the ICO and follow the requirements of GDPR. Above we make a recommendation that TPPs accessing any Smart Data should be accredited to the same standards as AISPs are for financial data.

BEIS may wish to consider whether other parties in the data chain accessing regulated datasets from TPPs should be required to demonstrate more robust standards of appropriateness than they currently are required to provide for under GDPR.

To provide some examples of what the various journeys might look like in practice, we follow Susan on her mission to make ends meet. Susan signs up for Bill Monitor App which is an Agent for Retrieve Data Co (an AISP). She then applies for a loan with Loan Co, but is rejected. So she applies for another loan using a credit broker, Credit BrokeMe. She gets a loan with Subprime Super Loan. They allow her to make flexible repayments based on her income. (Separately, she's also just got some two for one offers in the post for a clothes shop she often visits).

Susan using a service provided by an Agent (all inside PSD2 perimeter)



Susan decides to set up a bill monitoring service with Bill Monitor App.

She sets up her account and notices that when she is asked to accept the terms and conditions of the service, it mentions a Privacy Notice.

The Privacy Notice (required by GDPR) explains it will use the services of Retrieve Data Co to access her bank account data.

Bill Monitor App Agent

Bill Monitor App has its own brand. It checks people's spending to see how they could save money on bills, subscriptions and general overspending.

It uses the services of Retrieve Data Co to provide the 'budget' part of its app Susan can see and action recommendations from.

Bill Monitor App uses the data from the TPP to assess where Susan can make savings.

Retrieve Data Co AISP (TPP) Data Exporter

Susan is redirected from Bill Monitor App to Retrieve Data Co so she can connect her bank accounts to the app.

Susan gives her explicit consent (required by PSD2) to Retrieve Co to access the data and populate her 'budget' on Bill Monitor App for 90 days.

Susan opens another window to check out the Retrieve Data Co in advance and sees a link to a Privacy Notice and its regulated status with the FCA at the bottom of the page. She closes the window.

BankyData source Data Exporter

When Susan connects her first bank account to Retrieve Data Co, she authenticates to prove who she is and to establish the connection.

Once established, Susan is redirected back to Retrieve Data and then back to Bill Monitor App

In this first journey, Susan is presented with a Privacy Notice by Bill Monitor App, the Agent of Retrieve Data Co. Retrieve Data Co also fulfils requirements for GDPR by providing access to a Privacy Notice on its website. In this scenario, Susan has been presented with two different Privacy Notices (and an explicit consent under PSD2 from Retrieve Data Co).

In the case of a data breach or other breach of GDPR by the Agent, it is likely Susan would have recourse to Retrieve Data Co. In turn, Retrieve Data Co may seek damages from the Agent via any contractual arrangements between them.

Susan using the services of a Third Party (Not Providing AIS)



Susan

Susan decides to apply for a loan with Loan Co.

She puts in her details and notices that when she is asked to accept the terms and conditions of the service, it mentions a Privacy Notice.

The Privacy Notice (required by GDPR) explains Loan Co will use transaction data provided by Retrieve Data Co with Susan's consent, and other data sources to check creditworthiness

Loan Co Third Party (Not Providing AIS)

Loan Co has its own brand. Once Retrieve Data Co has passed transaction data to Loan Co it performs its credit worthiness check.

Loan Co uses Retrieve Data Co to access the transaction data on its behalf.

Loan Co uses the transaction data and other sources of data it has from the Credit Reference Bureau to assess creditworthiness

PSD2 perimeter I▶

Retrieve Data Co AISP Data Exporter

Susan is redirected from Loan Co to Retrieve Data Co so she can connect her bank account and Credit Card to Retrieve Data Co. Susan gives her explicit consent (required by PSD2) to Retrieve Data Co to access the data for 1 day.

Retrieve Data Co offers Susan the opportunity to open an account with Retrieve Data Co and see the data she has shared with Loan Co. She goes ahead and is presented with a dashboard that reminds her she's sharing data via Retrieve Data Co with Bill Monitor.

Susan's Retrieve Data Co dashboard has a link to the company's Privacy Notice in the menu.

Banky

Data source Data Exporter

Credity Card
Data source
Data Exporter

Susan connects her bank account to *Retrieve Data Co*. She authenticates to prove who she is.

Once established, Susan is redirected back to *Retrieve Data Co. Retrieve Data Co* ask if she would like to connect any other accounts, so Susan gives her explicit consent again.

She is redirected to *Credity Card* and authenticates to establish the connection.

In this second journey, Susan is presented with a Privacy Notice as part of her relationship with Loan Co, the Third Party (Not Providing AIS). Susan has already accessed services from Retrieve Data Co and so it is not required to provide the Privacy Notice again. However, since Susan has now accessed a consent dashboard it is provided in the menu for ease of reference. In addition Retrieve Co also provides a display of Susan's data in accordance with its requirements under PSD2.

In the case of a data breach or other breach of GDPR, Susan would need to identify the party she thought was at fault. Susan could complain to either party. If Susan struggles to get the complaint addressed by either Loan Co or Retrieve Data Co, she could take her complaint to the Financial Ombudsman Service (FOS). It is unclear how FOS would award redress, even if it finds, with the ICO, that her complaint is upheld and one of the parties is at fault.

Susan using the services of a Third Party (Not Prov AIS) and Fourth Party (Not Prov AIS) Credit BrokeMe **Retrieve Data Co Banky** Third Party AISP (TPP) Data source (Not Providing AIS) Data Exporter **Data Exporter** 'legitimate interests' Credit BrokeMe has its own Susan's application to Susan is redirected from Credit Susan connects her first bank Loan Co is refused so she brand. It gathers data on BrokeMe to Retrieve Data Co account to Retrieve Data Co, so she can connect her bank account to Retrieve Data Co. tries a credit broker, Credit share with potential she authenticates to prove who loan providers. BrokeMe. Susan is offered she is and to establish the a loan by Subprime Super Loan. It can provide ongoing Susan gives her explicit consent (required by PSD2) to Retrieve Co to access the data access to data to help its Once established, Susan is lenders ensure their loans continue to meet regulatory They offer her flexible redirected back to Retrieve repayments which match her income. Susan is presented with Privacy Data and then back to Credit requirements for affordability immediately opens Susan's BrokeMe. dashboard It also provides insights Notices by both Credit BrokeMe and Subprime about Susan's spending to a marketing company also mentioned in its Privacy It provides a display of the data it is sharing with Credit BrokeMe and a dashboard that Super Loan. reminds her she's also sharing Subprime Super Loan data via Retrieve Co with Bill Monitor, and did a one-off data share with Loan Co. performance of contract' Susan's Retrieve Data Other lender(s) dashboard has a link to the company's Privacy Notice in Marketing the menu. PSD2 perimeter I▶

In this third journey, Susan is presented with a Privacy Notice as part of her relationship with Credit BrokeMe, the Third Party (Not Providing AIS). Susan can access the Privacy Notice for Retrieve Data Co through her dashboard. In addition Retrieve Data Co provides a display of Susan's data in accordance with its requirements under PSD2. Retrieve Co has chosen to provide additional value by offering a consent dashboard. Susan can see the other arrangements which she has in place to share data on an ongoing basis. Helpfully, Retrieve Co has also listed the one-off data share she did with Loan Co and the date it took place.

As part of its legal basis for processing data, Credit BrokeMe accesses data about Susan from a few different sources, including Retrieve Data Co. (It would like to access information about her utility payments and fuel usage to provide a more robust view of Susan's outgoings and to consider whether it should start offering bill monitoring services too. Retrieve Co has said it is in discussions with an energy provider about accessing this data via the new Smart Data Right.)

Credit BrokeMe pulls together a data file on Susan and sends it out to a series of lenders. Subprime Super Loan bids for the loan and Credit Brokeme introduces Susan. Subprime Super Loan, the Fourth Party (Not Providing AIS), presents her with a Privacy Notice.

In her explicit consent to Retrieve Data Co, Susan agreed to continue sharing her data with Credit BrokeMe for a year. Ongoing access to Susan's data allows Subprime Super Loan to continuously assess how affordable the loan is for Susan. Subprime Super Loan adjusts the repayment schedule to meet Susan's income and expenditure. When it's Christmas, Susan pays a bit less.

Credit BrokeMe explains in its privacy policy that it also provides personalised insights about Susan to other companies that it thinks Susan has an interest in, based on her data. One of Susan's preferred shops sends her some offers to use over Christmas.

Subprime Super Loan explains in its privacy notice that its basis for processing Susan's data in this case is the 'performance of contract'. This is a different legal basis from the one that Credit BrokeMe used in its privacy notice when she agreed to share data with it. Susan no longer has a right to object to the processing of data because it is required to facilitate her contract (particularly, the flexible payments aspect of the contract).

After 90 days, Susan forgets to re-authenticate her connection with Credit BrokeMe. She receives an email from Subprime Super Loans that it can no longer provide her with flexible repayments. Because it cannot access her data any longer, Subprime Super Loans also says that it will have to foreclose on this loan, but can replace it with another immediately. Unfortunately, it is a higher rate of interest. Susan pays a fee for a late re-authentication and quickly takes the option to re-authenticate with Credit BrokeMe. She receives some more vouchers from her favourite shop.

In the case of a data breach or other breach of GDPR, in the first instance, Susan might be encouraged to complain to the relevant company first³³. It would be impossible for Susan to tell which company may have had the data breach, given how many companies Retrieve Co has shared data with; and how many entities Credit BrokeMe is onward sharing to. In the case of financial services, Susan would have a right to take her complaint directly to FOS. Although the credit broker and lender are outside of the PSD2 perimeter, they are caught by other regulations within the FCA perimeter.

However, it is unclear how FOS would assess the complaint. Susan may have shared with other AISPs and created other data chains that might require investigation. Traceability diminishes the further data is shared. The provider in this example with most visibility is the Third Party (Not Providing AIS) not the AISP which is the regulated party. The problem is exacerbated when an AISP uses a TSP to retrieve the data for it on its behalf. What happens if there is an interception of data as it moves?³⁴

Some of those in the chain, like the marketing company, may be outside of the FOS perimeter. FOS may not have jurisdiction to make requests. It is likely it would have to work with the ICO to agree a joined up approach to addressing the problem. In the event, the complaint was one that FOS felt was not within its purview, the ICO may not be able to help the consumer further on an individual basis. As we noted earlier, there is no data ombudsman or easy, free, access to individual redress.

Another observation from this journey is the considerable burden placed on Susan to read and engage in multiple Privacy Notices. Susan is unlikely to do this thus making these Privacy Notices somewhat ineffective.

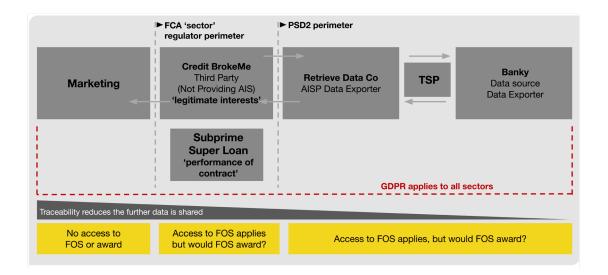
Further consideration could be given to the role of the TPP in acting as a 'data custodian' helping Susan to make sense of what it means to share her data with CreditBrokeMe. Currently TPPs are not incentivised to provide such value-add services because they provide a paid-for service to Agents or Third Parties Not Providing AIS, whose interests consequently come first. It is also unlikely that consumers would be willing to pay for this kind of help based on their existing rational disengagement.

³³ https://www.forbessolicitors.co.uk/personal/data-breach-claims.htm

³⁴ The Blueprint for Open Finance in the UK, FDATA, 2019 (1st edition)

This could mean the role of the TPP as the 'data custodian' may not materialise commercially.

BEIS should explore further the concept of a 'data custodian' or 'data facilitator' and the types of services it could require of TPPs in this role. Giving such TPPs a duty to put consumer's interests first would help balance their commercial interests. BEIS could usefully draw on existing work by Ctrl Shift on its Data Mobility Infrastructure Sandbox³⁵ to explore this concept further.



Preconditions for redress

Data portability in GDPR applies to personal data which an individual has provided to a firm. There are no strict definitions provided. However, there are three clear categories:

- Customer data (e.g. name, address etc)
- Data generated as a result of interaction with the service (e.g. transaction data, Smart Meter data, fitbit data)
- Additional data (inferred data) based on the data which an individual has provided. FDATA call this 'Value-added customer data'. It includes credit scores etc.

The right to data portability applies to points 1 and 2 but does not apply to point 3. However, a consumer could still request data held by them under point 3 as part of a subject information request³⁶.

While these categorise feel intuitively neat, there is still some uncertainty³⁷.

These definitions do not take account of the dynamic nature of data sharing and how personal data may be used to continue to 'feed' insights. Inferred data may create an 'asset' about an individual which is static, based on previously shared data; or dynamic, based on a continual feed of data.

³⁵ https://www.ctrl-shift.co.uk/wp-content/uploads/2019/06/DMIS_June_2019_Downloadable_Singles_Final4.pdf

^{36 &#}x27;What does provided by a Controller mean?' https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-data-portability/

³⁷ See Appendix 1, Data Mobility Report, 2018, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/755219/Data_Mobility_report.pdf

The assessment of the nature of data is important because a precondition for calculating redress in the case of a data breach must include how data is valued.

The assessment of harms in Chapter 2 shows that there are a number of reasons why consumers may be due redress. In considering redress for data breaches³⁸, further research is required to assess:

- how data itself is valued in a variety of permutations
- how silent party or inferred sensitive data may be adequately protected
- how distress or reputational damage might be assessed

Any calculation of the quantum of redress would be required to take these issues into account, alongside the role of the participant in the data chain.

"If Party A (being an end customer) and party B (being an end customer) both have the same volume of data hacked from a TPP application but where Party A has data that reveals an embarrassing habit and where party B does not have an embarrassing habit revealed, does Party A, having suffered a greater loss, have an entitlement to a larger claim?"39

Conclusion

The complexity of PSD2 participant roles and the data chains they can create make the assessment of liability and the apportionment of redress challenging. The bedrock of Smart Data should be a clear liability regime which can define the participants in the data chain; their responsibilities and liabilities; and how redress will be apportioned in the event of GDPR failings and particularly, data breaches. Specifically to provide for redress a regulator/ombudsman would need to:

- Identify participants in the data sharing journey
- Identify which participants hold the data, for what time period and for what purpose
- The party that is responsible for the breach of GDPR
- Have jurisdiction for enforcing against the participant
- Facilitate a way for firms to manage disputes and communicate to the Ombudsman

To address these issues, we have previously suggested giving sector regulators concurrent powers for data protection. This could help address cases inside the perimeter where the ombudsman would have jurisdiction. However, it does not address cases where:

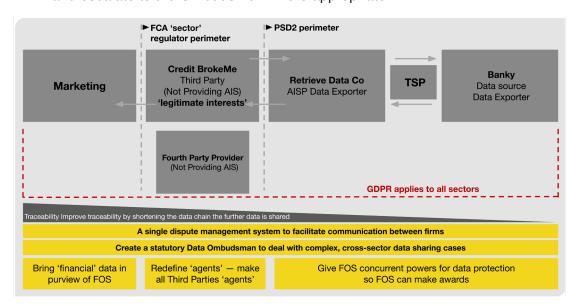
- TPPs access data across multiple regulated sectors, or
- TPPs share outside the regulatory perimeter, or
- TPPs access data across multiple regulated sectors and onward share outside the regulatory perimeter.

^{38 &}quot;A data breach is when personal data is lost, destroyed, accessed or disclosed in an unauthorized way whether that's by accident or deliberately by someone inside or outside the organisation" https://www.forbessolicitors.co.uk/personal/ data-breach-claims.htm

³⁹ The Blueprint for Open Finance in the UK, FDATA, 2019 (1st edition)

In these cases, we suggest BEIS undertake further work to consider some potential remedies. Suggestions for further investigation include:

- A duty on the TPP to put consumer interests first before those of
 the parties that pay the TPP for access to the consumer's data. This
 could include provision of key value added services such as consent
 management tools, clarity about the display of 'consolidated data' and
 provision of labels to help consumers better understand the impact of
 onward sharing.
- Giving sector regulators concurrent powers for data protection so data breaches within the perimeter can be addressed by sector Ombudsmen
- The extension of the regulatory perimeter to include sector data
 (e.g. financial data, energy data or telecoms data) used by parties
 outside the regulatory perimeter. In such cases, these unregulated
 parties would be subject to investigative powers by sector regulators
 and Ombudsmen in relation to the data processed by the party where
 a breach was suspected.
- The introduction of a single Data Ombudsman for complex, crosssector data sharing cases. This Ombudsman would work in partnership with sector ombudsmen to provide advice and the final say in disputed cases.
- Simplifying the PSD2 architecture for Smart Data by bringing
 Third Parties (Not Providing AIS) and Technical Service Providers
 into the regulatory perimeter. TSPs would be regulated as existing
 AISPs are. Third Parties (Not Providing AIS) could become 'Agents'
 (with a revised definition of 'Agent'). By making these firms 'agents' of
 the TPP, this would focus the liability on the TPP in the event of
 problems downstream.
- Exploring the concept of loading liability for the onward share data chain onto TPPs so that they become responsible for managing traceability and the conduct of firms to whom data is onward shared. This could cause some natural reduction in the data chain and make apportioning redress easier.
- A single, accessible Dispute Management System to facilitate firms communication to resolve problems, agree apportionment of blame and escalate to the Ombudsmen where appropriate.



Biographies

Miles Cheetham



As Head of Proposition at The Open Banking Implementation Entity (OBIE) since its inception in 2016, Miles has been responsible for understanding what consumers want from open banking enabled services, acting as the voice of the customer across the programme.

He led the development of the ground-breaking and highly regarded Customer Experience Guidelines, a key part of the Open Banking Standard, which focuses on consent and customer authentication as central to the data sharing journey. This was achieved through extensive engagement with the market, customer interest groups and primary

customer research. He has deep experience of customer-led digital product development across banking & telecoms. Prior to joining OBIE he worked in senior product development and strategy roles for major brands including Vodafone, MTN Group, Sky and Verizon.

Sharon Cunliffe



An experienced lawyer specialising in data privacy, with deep expertise in the General Data Protection Regulation (GDPR) as well as financial services regulation.

Sharon has until recently been leading legal and regulatory support in payment services and data privacy at the OBIE, with a particular interest in data privacy and the regulatory and statutory challenges that data privacy is currently presenting at domestic and European level both in the context of payment services and data privacy on a standalone basis. She engages with the Information Commissioners Office (ICO), the

Financial Conduct Authority (FCA) and government departments (e.g Department for Digital, Culture, Media & Sport (DCMS) to find practical solutions arising out of challenges and conflicting statutory provisions contained within both PSD2 and GDPR.

Biographies

Faith Reynolds



Faith Reynolds advises regulators and industry on technology, innovation and business conduct in the financial services market. She is Independent Consumer Representative for the Open Banking Implementation Entity, significantly influencing policy, design and implementation of the trust framework, consent flows and dashboards.

Gavin Starks



On behalf of HM Treasury, Gavin co-chaired the development of Open Banking Standard, leading banks, trade associations, startups, regulators and consumer rights organisations to lay the foundations for new regulation.

He has worked with public and private sector organisations internationally, with Ministers, C-suite leaders and startup founders. He was the founding CEO of the Open Data Institute, has sat on the GLA Smart London and the Ministry of Justice Data Science and Evidence boards and provided evidence to a Parliamentary Select Committee on

'Big Data'. As a serial entrepreneur he has cocreated over a dozen companies, creating economic, environmental and social impact. His work has led to recognition as one of the most influential people in data, awards for innovation and expertise, and frequent international presentations on innovation, the web of data and its impact on society.

Biographies 45

Appendix:

GDPR principles, data rights and triggers

GDPR Principles

Article 5(1) requires that personal data shall be:

"(a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');

- (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
- (c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- (d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) adds that:

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."40

⁴⁰ https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/

Data Rights under GDPR and their trigger points:

Some rights under GDPR overlap and at times, even when they are triggered, GDPR permits Controllers to use an alternative right if it achieves the same outcome. There are also many exemptions which are permitted both under GDPR and DPA 2018 and Controllers may be able to rely on one of those when responding to a right request.

Right	Trigger	Notes
Be informed	Prior to any processing taking place - Privacy Notice	A consumer is entitled to mandatory information about the collection and use of their personal data before processing of the data takes place.
Access (also known as a SAR)	Anytime but right only applies against a Controller	A consumer can (verbally or in writing) ask an organisation whether or not they are using or storing your personal information. In addition, they can ask for copies of the personal information. A consumer is entitled to know, what an organisation: • holds • how they are using it; • who they are sharing it with; and • where they got the data from.
Rectification	Where data held by an organisation is inaccurate or incomplete	A consumer has the right to ask for their data to be corrected, make complete (or deleted)

Erasure/ Deletion

(also known as right to be forgotten)

(qualified right)

The organisation no longer needs the data for the original reason they collected or used it for.

Consumer initially consented to the organisation using the data, but have now withdrawn their consent.

Consumer objects to the use of their data, and their interests outweigh those of the organisation using it.

Consumer has objected to the use of your data for direct marketing purposes.

The organisation has collected or used consumer data unlawfully.

The organisation has a legal obligation to erase the data.

The data was collected from the consumer as a child for an online service.

In some circumstances, a consumer can ask an organisation to delete that data.

Restrict (qualified right)

Consumers have the right to request you restrict the processing of their personal data in the following circumstances:

- contests the accuracy of their personal data and the organisation are verifying the accuracy of the data;
- the data has been unlawfully processed (ie in breach of the lawfulness requirement of the first principle of the GDPR) and the consumer opposes erasure and requests restriction instead:
- It is no longer needed the personal data but the consumer needs the organisation to keep it in order to establish, exercise or defend a legal claim; or
- the individual has objected to you processing their data and the organisation is considering whether there are legitimate grounds override those of the consumer.

In some circumstances, Consumers have the right to request the restriction or suppression of their data. When processing is restricted, organisations are allowed to store the personal data, but not use it.

This right has close links to the right to rectification

Portability (qualified)	the right only applies to data that: • is held electronically, and • the consumer has provided to the organisation.	In some circumstances, a consumer has the right to ask for the transfer of their data to another organisation in a way that is accessible and machinereadable. Organisations must do this if the transfer is, "technically feasible".
Object	 a task carried out in the public interest; the exercise of official authority; for their legitimate interests; scientific or historical research, or statistical purposes; direct marketing 	A consumer can stop or prevent the organisation from using their data.
Rights in relation to automated decision making and profiling	Organisations are only permitted to solely carry out automated decision making if the decision is: • necessary for entering into or performance of a contract between the organisation and the consumer; • authorised by law (ie fraud purpose orr tax evasion); or • based on the individual's explicit consent. Where organisations are using special category personal data,, processing is only permitted with: • consumers' explicit consent; or • the processing is necessary for reasons of substantial public interest.	requires organisations to give consumers specific information about the processing; obliges organisaitons to take steps to prevent errors, bias and discrimination; and gives consumers a rights to challenge and request a review of the decision.

risk	Access to shared data creates new operational & execution risks for firms	execution	Use of data creates market and systemic risks		Vide sharing of data exacerbates and risks to society	Wide sharing of data exacerbates consumer harm and risks to society
Access to data: is data easily accessible, accurate from the dup to date? IT systems: Do firms have it from the right systems in place to facilitate new tech? Are they Lesilient? Is investment is proportionate? Performance of technology: It is the tech working, reliable from and consistently available? It and consistently secure in transit? Could data be intercepted in transit? Is data an encrypted? Secure transfer of data: is it A consistently secure in data be intercepted in transit? Is be data encrypted? Is data secure at all ends of the data chain? Testing facilities: do firms thave access to facilities for testing?	Data governance: do firms follow ICO guidelines? Can they control data in the cloud? Do they have the right oversight? Liability and insurance: Is the data traceable? Is liability between parties clear? Is there a dispute management system? Can firms access and claim on insurance effectively? Data security and breaches: is it safe and secure? Effective anonymisation? Algorithmic bias, discrimination and transparency: how has it been tested and audited? Is there over-confidence in it? Data driven automation: is there human oversight? Appropriate skills and expertise: can firms effectively manage new tech and outsourcing?	Managing data: is it clean, sorted and stored properly? Are its attributes and linking accurate? Sensitive and silent party data: how is data categorised and attributed? Accuracy and comprehensiveness: how is it categorised? Is data accurate and comprehensive? Blurring regulatory perimeter: is it clear what regulations are applicable and how it's supervised? Ethical challenges: what additional considerations are required when using or merging different sets of data? Commercial confidentiality: can SMEs rely on confidentiality? How does data sharing affect commercial espionage? Can data be de-anonymized?	Nefarious actors: what are the incentives and routes in for illegitimate actors? How is fraud monitored and guarded against? What's the likelihood of cyberattacks? Network effect: how does the amount of data entrench incumbents or reduce competition? Access to technology: can consumers access services? Digital exclusion? How often are software or hardware updates required? Misconduct and incompetence: do firms follow the rules and incompetence: do firms follow the rules and standards? Do they use the data purposes other than the consumer agreed to? Business models prevail and create barriers to alternatives? Market discipline: what reporting and accountability requirements are there? Is there sufficient oversight, supervision and enforcement? Are there	Consumer expectations of data usage: do consumer trust data sharing? Does the trust data sharing? Does the trust data sharing? Does the pricing of the product? there adequate price expectations? Can they make choices effectively? Misleading: is data out of date, inaccurate or incomprehensive so insights and advice are wrong? Product design features: are incomprehensive so insights and advice are wrong? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Product design features: are profilerate? Do firms update in a timely way? Switching does data sharing make it harder	ow he ct? Are se d and d and s? Do groups groups groups tion groups groups and tier? tier	Social scoring: do firms or government create scores for people or businesses which reduce access, choice, social mobility, aspiration or democracy? Price optimisation: does personalisation lead to an increased loyalty penalty? Are consumer behaviours exploited? Communications: are people and businesses aware of their rights and responsibilities? Complaints and redress: can consumers access justice and recompense? Red lining and exclusion: are individuals, communities or groups of people excluded? Privacy and liberty: does the products limit or reinforce past consumer behaviours, reduce choice or remove privacy? Are human rights harmed?

Societal risk

Consumer harm

Market / systemic risks

Execution risks

Operational risks

Glossary & terminology

Term	Definition	
AISP	Account Information Service Provide. rln this report an AISP is a type of TPP.	
Agent	Regulated AISPs (Principals) can have agents, providing services on behalf of the principal.	
ASPSP	Account Servicing Payment Service Provider (for example Bank, Building Society acting as the Data Source)	
Controller	Data Controller (GDPR)	
CMA	Competition Markets Authority	
CRA 2015	Consumer Rights Act 2015	
C1, C2, C3	(Data) Controller 1, Controller 2 etc.	
DPA 2018	Data Protection Act 2018	
DS	Data Subject	
FCA	Financial Conduct Authority	
FPNPA	Fourth Party Not Providing AIS	
GDPR	General Data Protection Regulation	
ICO	Information Commissioner's Office	
LB	Lawful Basis	
LI	Legitimate Interest (as a lawful basis under GDPR)	
PD	Personal Data	
PISP	Payment Initiation Service Provider. In this report a PISP is a type of TPP	
PN	Privacy Notice	
PoC	Performance of Contract (as a lawful basis under GDPR)	
Processor	Data Processor (GDPR)	
PSD2	Second Payment Services Directive	
PSRs	Payment Services Regulations 2017	
TPP	Third Party Provider. In this report we use the term to mean a TPP which is accessing data like an AISP. In PSD2 a TPP can also be a PISP which initiates payments.	
TPNPA	Third Party Not Providing AIS	

Acknowledgements

With thanks to Galina Carroll, Daniel Jenkinson and Gavin Littlejohn for their input

Limit of Liability and Disclaimer of Warranty

The authors, researchers and contributors have used their best efforts in preparing this work. Dgen Network Limited makes no representation or warranties with respect to the accuracy or completeness of the contents of this worl and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose and shall in no event be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential, or other damages.

Trademarks: all trademarks are acknowledged.

Glossary & terminology 51

52 Glossary & terminology

Contents 53